

NAVAL WAR COLLEGE
Newport, R.I.

JOINT C4I INTEROPERABILITY: A LONG HISTORY, A TENUOUS FUTURE

by

Patrick J. Kanewske
Lieutenant Colonel, USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

7 May 2002

Faculty Advisor
Captain David J. Maresh, USN

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207		
8. Title (Include Security Classification): JOINT C4I INTEROPERABILITY: A LONG HISTORY, A TENUOUS FUTURE (UNCLASSIFIED)			
9. Personal Authors: Lieutenant Colonel Patrick J. Kanewske, USMC			
10. Type of Report: FINAL	11. Date of Report: 7 MAY 2002		
12. Page Count: 21	12A Paper Advisor (if any): Captain David J. Maresh, USN		
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: Command, Control, Communications, Computers, and Intelligence (C4I); Interoperability; C4I Systems; JTF Commander; Defense Information Systems Agency (DISA); Information Technology (IT); Joint Interoperability Test Command (JITC); Stovepipes; Operational Factors			
15. Abstract: DoD has been confronted with interoperability problems for more than 30 years, and achieving effective C4I interoperability continues to be a difficult matter for DoD to resolve. Through the years DoD has issued increasingly assertive interoperability policy guidance, strengthened procedures associated with reviewing system requirements and making acquisition decisions, and attempted to field systems that will help ensure C4I interoperability. However, these initiatives have failed to ensure the operational commander is provided C4I systems that are interoperable.			
The haphazard fielding of service-unique C4I systems must stop. Technology is available to ensure the operational commander receives interoperable C4I systems for use on the battlefield. The solution to the C4I systems quandary is interoperability assurance. A critical element of interoperability assurance is a clear prescription of a common suite of capabilities that must be inherent in all C4I systems that desire to interoperate. At each level of interoperability, DoD must identify a common suite of capabilities across procedure, applications, infrastructure, and data that must be incorporated by system developers in order to have a common-ground basis for Joint interoperability assurance. Common standards must also be adhered to for each capability.			
Leadership at the highest levels in DoD must leverage current initiatives and institute a process to ensure that the Regional CINCs have the interoperable C4I systems they require to fight and win the nations battles. Interoperable C4I systems must be fielded as a hedge against friction on the battlefield.			
16. Distribution / Availability of Abstract: X	Unclassified	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461	20. Office Symbol:	C	

Abstract

JOINT C4I INTEROPERABILITY: A LONG HISTORY, A TENUOUS FUTURE

The Department of Defense has been confronted with interoperability problems for more than 30 years, and achieving effective Command, Control, Communications, Computer, and Intelligence (C4I) interoperability continues to be a difficult matter for DoD to resolve. Through the years DoD has issued increasingly assertive interoperability policy guidance, strengthened procedures associated with reviewing system requirements and making acquisition decisions, and attempted to field systems that will help ensure C4I interoperability. However, these initiatives have failed to ensure the operational commander is provided C4I systems that are interoperable.

The haphazard fielding of service-unique C4I systems must stop. Technology is available to ensure the operational commander receives interoperable C4I systems for use on the battlefield. The solution to the C4I systems quandary is interoperability assurance. A critical element of interoperability assurance is a clear prescription of a common suite of capabilities that must be inherent in all C4I systems that desire to interoperate. At each level of interoperability, DoD must identify a common suite of capabilities across procedure, applications, infrastructure, and data that must be incorporated by system developers in order to have a common-ground basis for Joint interoperability assurance. Common standards must also be adhered to for each capability.

Leadership at the highest levels in DoD must leverage current initiatives and institute a process to ensure that the Regional CINCs have the interoperable C4I systems they require to fight and win the nations battles. Interoperable C4I systems must be fielded as a hedge against friction on the battlefield.

OPERATIONAL PERSPECTIVE

Joint force employment has become the norm for U.S. military operations, and will likely remain so. The effectiveness and efficiency of future operational commanders will depend, to a great degree, on the level and nature of interoperability between the Service elements of the Joint Task Force (JTF). The Department of Defense has been confronted with interoperability problems for more than 30 years, and achieving effective Command, Control, Communications, Computer, and Intelligence (C4I) interoperability continues to be a difficult matter for DoD to resolve. Through the years DoD has issued increasingly assertive interoperability policy guidance, strengthened procedures associated with reviewing system requirements and making acquisition decisions, and attempted to field systems that will help ensure C4I interoperability. However, these initiatives have failed to ensure the operational commander is provided C4I systems that are interoperable.

Some view the problem as one related to the huge increase of C4I systems on the market due to the increased technology associated with the Information Technology (IT) revolution. The claim is that C4I systems interoperability is as good as it gets, and DoD simply needs to keep fielding the latest technology to stay on top of the demand to communicate, and collect, process, and store information. Others view technology as the answer to the C4I interoperability dilemma, and that the latest technology has the means to either verify systems are interoperable before they are fielded or ensure the infrastructure on which the systems pass information is designed to ensure C4I systems interoperability. Whatever the case, the highest levels of DoD leadership must take an active role in ensuring the nation's precious resources are spent on the proper equipment for the operational commander. This paper will argue that the haphazard fielding of service-unique C4I systems must stop and that technology is available to ensure the

operational commander receives interoperable C4I systems for use on the battlefield. The operational factors of space, time, and force will be examined as they relate to fielding interoperable C4I systems as a hedge against friction on the battlefield.

HISTORICAL PERSPECTIVE

Joint Publication 1 states “the nature of modern warfare demands that we fight as a team... Joint force commanders choose capabilities they need from the air, land, sea, space and special operations forces at their disposal... Joint warfare is essential to victory.”¹ Joint Publication 1 gives the impression that the requirement for interoperability is new, and that the Armed Forces should incorporate this new requirement into their planning. This is misleading. Efforts to improve interoperability began with the establishment of the Joint Army and Navy Board in 1903. Table I provides an overview of the major actions taken to help improve interoperability between the Services since the Joint Army and Navy Board.

Although the need to conduct Joint operations has long been recognized, the U.S. has a mixed record of success with interoperability. World War II showed that command of Joint operations by mutual cooperation left much to be desired. Although the command structures and operating techniques developed during the war were effective in defeating the enemy, changes were clearly required to codify the ad hoc procedures that made victory possible. Command structure was seen as the tool to restrain service parochialism and increase interoperability. Many of the lessons learned about the advantages of interoperability in World War II were forgotten in the Korean conflict and subsequently not addressed in Vietnam. More recently, in operations like the Iranian Hostage Rescue Attempt and URGENT FURY in Grenada, the services had not incorporated interoperability lessons learned into their planning. Although

¹ Department of Defense, Joint Chiefs of Staff, *Joint Warfare of the Armed Forces*, Joint Publication 1 (Washington: National Defense University Press, 1991), iii.

Action	Year	Purpose
Joint Army and Navy Board ²	1903	Mandated that the Army and Navy coordinate their actions as to produce the most effective mutual support and attain coordination in operations.
National Security Act ³	1947	Secretary of Defense first named to coordinate the activities of the Departments of War, Navy, and Air Force. Codified the Joint Chiefs of Staff.
National Security Act of 1947 Amended ⁴	1949	Created the Department of Defense and subordinated the three service secretariats to the Defense Secretary. Command structure was seen as the tool to restrain service parochialism and increase interoperability.
Defense Reorganization Act ⁵	1958	Removed the operational authority of the service chiefs, thus creating an atmosphere for interoperable operations.
Goldwater Nichols Act ⁶	1986	CJCS was designated as the principal military advisor to the NCA. Unified Commanders were specifically given operational control of the forces within their AOR. Requirements for Joint officer assignment and education were established.
Joint Publication 1 ⁷	1991	States Joint warfare is essential to victory and that interoperability is indispensable to conducting Joint operations.

Table I. Actions Taken to Help Ensure Joint Interoperability

Operation DESERT STORM exercised many of the provisions set down to improve interoperability, the services experienced interoperability shortfalls related to the Air Tasking Order, in particular. Serious technical problems and service autonomy have historically prevented the services from operating with one another.

The defense reorganizations were intended to improve interoperability by creating centralized command structures that would enforce unity of effort. The record of joint operations in the last fifty years shows that interoperability problems have continued despite the

² Joint Army and Navy Board, *Joint Action of the Army and the Navy* (Washington: Government Printing Office, 1927), iv.

³ Russell Weigley, *The American Way of War*, (Bloomington: Indiana University Press, 1973), 374.

⁴ *Ibid.*, 374.

⁵ Congress, Senate, *Congressional Record*, 99th Congress (3 October 1958)

⁶ Department of Defense, Armed Forces Staff College, *The Joint Staff Officer's Guide 1991*, AFSC Publication 1 (Washington: Government Printing Office, 1991), 2-11.

⁷ Department of Defense, Joint Chiefs of Staff, *Joint Warfare of the Armed Forces*, Joint Publication 1 (Washington: National Defense University Press, 1991), iii.

attempt to increase command centralization. Defense reorganizations have not improved interoperability because they only treated a symptom of the actual problem: the lack of routine operational interaction between the services. Despite the statutory divisions and separate roles and missions that have largely prevented operational interaction between the services throughout U.S. history, there are currently preventable technical aspects affecting the joint interoperability problem. The Services have historically developed their own C4I systems. The legality of this policy will be discussed later, but suffice it to say that these “stovepipe” systems have created enormous technical interoperability problems for the Services. The following technical and procedural problems have prevented interoperability in the Armed Forces⁸:

- No joint firewall policy.
- Global Command and Control System (GCCS) is not interoperable between the Services.
- Bandwidth is not sufficient for GCCS traffic.
- No coordination of plans.
- Different message formats.
- Warfighting levels not distinct.

Realizing the magnitude of these problems, the Assistant Secretary Defense (ASD) for C4I stated the following in a speech to the Communications and Electronics Association on August 22, 1995:

“We have been burned in the past by the acquisition of vendor proprietary systems that represented the best value for the money at the time, but whose upgrades proved too costly as time and technology advanced. We have learned our lessons – standardize the interfaces, using commercial standards whenever possible to create a systems environment in which individual creativity can flourish, so the component software and hardware systems can rapidly evolve and be integrated into a stable matrix of interoperable systems at minimum cost and downtime. Competing vendors often inject proprietary designs in their products without regard to interoperability standards, which then render them incompatible with other network components. Competition among firms developing similar technologies is fierce... It is a known fact that DoD still has a sizable inventory of C4I systems that are legacy in nature and stovepiped in function, as they do not interoperate with other systems. In October 1993, Deputy Secretary of

⁸ Rick Lynch, et al, *U.S. Army and Marine Corps Interoperability: A Bottom-up Series of Experiments*, (Alexandria, VA: Joint Advanced Warfighting Program, 2000), 7-18.

Defense Perry imposed a three-year deadline to minimize the number of duplicative DoD information support systems and make the remaining migration set interoperable.”⁹

Mr. Paige understood the interoperability problem, but either did not know how or did not have the will to effect the changes required to solve the problem.

CURRENT PERSPECTIVE

Ironically, the same advances that are enhancing the capabilities of C4I systems to access and exchange information are also compounding the challenge to field systems that can interoperate with each other at comparable levels of sophistication, thus reducing the operational commander’s ability to realize the full benefit of today’s technology. The rapid evolution of information technology is providing the systems developer with many product choices that offer similar functional capabilities, yet few of these choices are interoperable with each other. In many cases, commercial industry is moving faster than the policy bodies can prescribe standards. Many vendors are vying to develop the Commercial Off The Shelf (COTS) standard of choice. Often, products are provided free to the marketplace as a strategy to achieve this objective. Also ironic is the tendency of DoD Services and Agencies to structure and regulate access within its C4I systems architectures, thus running the risk of inhibiting its ability to access critical information across the global information enterprise.

DoD Services and Agencies are making progress to improve C4I systems capabilities and interoperability. In addition, many DoD-wide efforts are underway to improve C4I systems interoperability.¹⁰ The Joint Technical Architecture (JTA) defines standards governing the implementation of system capabilities and interfaces. The goal of the Defense Information Infrastructure (DII) Common Operating Environment (COE) is to establish a commonly defined

⁹ Emmett Paige, Jr., *Retaining the Edge on Current and Future Battlefield Defense*, Defense Issues, (August 1995), 4.

executable environment for systems. This environment is intended to drive developers toward a common set of solutions that work together and that compliment each other. The DII Master Plan is meant to ensure that an infrastructure is in place to allow for the establishment of a common link between systems as they develop. The Shared Data Environment (SHADE) is intended to reach agreement on common data models for systems. The Joint Interoperability Test Command (JITC) tests and certifies systems based on standards conformance and demonstrated application-to-application interoperability. The Joint Battle Center is a forum for conducting experiments regarding information systems interoperability, integration, technology insertion, and system performance in a Joint environment.

However, while all of these initiatives are important in the fight for interoperability assurance, they are not sufficient. Leadership at the highest levels in DoD must leverage current initiatives and institute a process to ensure that the Regional CINCs have the interoperable C4I systems they require to fight and win the nations battles.

Operational C4I requirements vary dramatically with respect to the degree of interoperability needed to respond appropriately. In some cases the need to exchange information between one node and another may simply involve transmitting an informal voice or text message. In other cases, more elaborate exchanges of information may be required that involve the need to disseminate multi-media information, or the need for the warfighter to collaborate simultaneously over a shared picture of the battlespace, or the desire for several arms of the JTF to author a decision brief jointly. DoD lacks a construct for ensuring the operational commander achieves interoperability at these different levels (environments) of operational sophistication.

¹⁰ C4ISR Architecture Working Group, *Levels of Information Systems Interoperability (LISI)*, 30 March 1998, http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdfdocs/lisi.pdf

At least three realities continue to inhibit the achievement of Joint interoperability across C4I system and Joint service boundaries. Figure 1 demonstrates how a common picture of these realities can help make interoperability a certainty. First, stovepipe systems (systems that do only one or limited applications or services) are the order of the day. DoD Services and Agencies focus on developing systems that enable functional applications and services, and address associated data considerations. Consequently, they do not adequately address the requisite infrastructure dimensions of a C4I system nor enable policies and procedures. Second, even when the Services and Agencies focus on the same enabling attribute, they may well have a different view of what specific capabilities are needed to achieve the same mature level of interoperability. In other words, system functions are also stovepiped. The systems capabilities simply do not interact in a Joint environment. Third, even when the Services and Agencies have focused on all of the enabling attributes and have agreed on the same set of capabilities within each attribute, there is still a tremendous margin for error because of the multitude of choices generally available for implementing each specific capability. Although the C4I systems may be standard compliant, they still might not be able to interoperate with each other, often due to the latitude in the standard itself. This latitude provides the Services and Agencies with freedom in interpretation and the incorporation of permissible options and capabilities. In addition, DoD has exacerbated the situation by allowing the Services and Agencies to circumvent the C4I interoperability certification process via an easy waiver process.



Figure 1. Making C4I Systems Interoperability a Certainty

LEGAL ASPECTS

In addition to ignoring the basic mandates of the National Security and Defense Reorganization Acts of the past, and their inability to leverage current interoperability initiatives, the Services are in violation of established procedures mandated in several DoD and CJCS Directives and Instructions, as well as the current National Military Strategy and Joint Vision 2020. The DoD Directives and Instructions provide clear guidance on the acquisition and maintenance of C4I systems to ensure interoperability. Table II provides details related to established interoperability rule sets.

Systems interoperability is high on the list of subjects discussed in the DoD acquisition program and throughout doctrine and policy documents. APPENDIX A provides a list of definitions and organizations, programs, systems, and exercises that deal with or are directly related to interoperability. The systems and organizations cause one to believe that DoD has a handle on the interoperability problem and is taking steps to ensure its benefits are realized by the Services. Unfortunately, this cannot be further from the truth.

Historically, systems interoperability has been more a matter of chance than deliberate planning and the services have used funds to satisfy immediate needs without considering DoD-wide interoperability issues. The DoD has had problems implementing its policies and procedures relative to C4I systems interoperability for joint military operations since it first issued related directives in 1967. Throughout the years, DoD has reemphasized its commitment to interoperability by issuing more specific directives and establishing a timeline to develop and field a Joint C4I architecture. Moreover, non-technical interoperability problems exist such as substantial variations within the Services regarding procedures, tactics, and rules governing operational aspects of warfighting. And service C4I interoperability initiatives were not unified

Directive/Instruction	Year	Content
DoD Directive 4630.5 ¹¹	1992	<u>Compatibility, Interoperability, and Integration of C3I Systems [Mandatory]</u> Establishes policy to develop, acquire, and deploy compatible, interoperable, and integrated C3I systems.
DoD Instruction 4630.8 ¹²	1992	<u>Procedures for Compatibility, Interoperability, and Integration of C3I Systems [Mandatory]</u> Assigns responsibilities and establishes procedures. DISA tasked as the single POC to identify and test C4I systems that require an interoperability capability and maintain a database of those systems that have the interoperability stamp.
CJCSI 6212.01A ¹³	1995	<u>Compatibility, Interoperability, and Integration of C4I Systems</u> Establishes detailed implementation procedures and responsibility - C4I for the Warrior is the objective vision.
National Military Strategy ¹⁴	1997	“Laying a solid foundation for interoperability with our alliance and potential coalition partners is fundamental to effective combined operations...”
Joint Vision 2020 ¹⁵	2000	“Interoperability is a mandate for the Joint Force of 2020...”
DoD Directive 5000.2-R ¹⁶	2001	<u>Operation of the Defense Acquisition System</u> Spells out the acquisition process as it relates to interoperability and provides specific details as to the establishment of systems interoperability Key Performance Parameters.

Table II. C4I Systems Interoperability Established by Law

because no common global vision existed to guide the future direction in support of the warrior during Joint operations.¹⁷ The Military Departments and the office of the Joint Chiefs of Staff have simply not carried out their responsibilities.

¹¹ DoD Directive 4630.5, *Compatibility, Interoperability, and Integration of C3I Systems*, (Washington: DoD, 1992), 2.

¹² DoD Instruction 4630.8, *Procedures for Compatibility, Interoperability, and Integration of C3I Systems*, (Washington: DoD, 1992), 6.

¹³ CJCS Instruction 6212.01A, *Compatibility, Interoperability, and Integration of C4I Systems*, (Washington: DoD, 1995).

¹⁴ Shalikashvili, *NMS*, 22.

¹⁵ *Joint Vision 2020*, (Washington: JCS, 2000), 15.

¹⁶ DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, (Washington: DoD, 2001), 7.

The Joint Staff's Director for C4 Systems (J-6) is assigned primary responsibility for ensuring compliance with the interoperability certification requirement. DISA's Joint Interoperability Test Command (JITC) is the sole certifier of C4I systems. According to Joint Staff guidance, commanders in chief, the services, and DoD agencies are required to adequately budget for certification testing. Certification is intended to help provide the warfighter with C4I systems that are interoperable and to enable forces to exchange information effectively during a joint mission. The requirement further states that a system must be tested against all systems with which it must interoperate. Briefly, DoD does not have an effective process for certifying existing, newly developed, and modified C4I systems for interoperability. As a result, many C4I systems have not been certified for interoperability and, in fact, DoD does not know how many require certification, and there is no plan to prioritize systems for testing.¹⁸ Bottom line, C4I systems currently receive approval for production and fielding even though they may have not been certified as interoperable.

OPERATIONAL IMPACT/CONSEQUENCES

A JTF that is not interoperable directly and negatively affects the Operational Factors of space, time, and force. Consequently, the JTF Commander is relegated to provide C4I system workarounds to compensate for the friction caused by the relationship between space and time, space and force, and time and force.

Factor Space

The ability of a JTF to possess C4I systems that interoperate directly correlates to the distance to the employment area and between points in the employment area. Interoperable

¹⁷ United States General Accounting Office, *DoD's Renewed Emphasis on Interoperability is Important but Not Adequate*, (Washington: GAO, 1993), 26-35.

¹⁸ United States General Accounting Office, *Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability*, (Washington: GAO, 1998), 1-2.

systems provide the commander the ability to communicate and send data over longer distances.

The operational commander's ability to electronically reach an Area of Responsibility (AOR) that is a great distance from his command post saves time, money, and increases the efficiency of command and control. Units in the AOR do not have to be concerned with staying close to one another if interoperable systems are employed. The result is a JTF with much greater influence over a larger space.

The relationships between space and force, and space and time are particularly critical. The ability of a force to work together often determines the area or space that force can influence. If a force's systems are interoperable and it is directly linked electronically with other forces in the area, then this Joint force has the ability to influence a larger space and in less time. Interoperability between the forces may also determine the geo-strategic position of the combatants. Their ability to operate with one another will determine if a maritime force or land force is employed, and the amount of time it takes that force to reach the AOR relative to their location in the world. The ability of the force to interoperate can also determine the location (in the space) the force is employed relative to the enemy.

Factor Time

Time is perhaps the most critical Operational Factor because space can be regained that has been lost and forces can be reconstituted, but time lost can never be recovered. Preparation time related to JTF training, planning, mobilization, and deployment can be reduced if the force is interoperable. Typically, precious time is wasted ensuring the systems that the Services bring to the fight have the ability to interoperate. CINC J6 personnel are tasked to ensure that service systems are interoperable before the task force deploys. Often they must find the best way to

make the systems work together, thus using up time that would otherwise be spent preparing to engage.

C4I systems interoperability can affect the relationship between time and force. The command and control cycle of decisions and actions on the battlefield can be reduced with adequately interoperable systems. This would help ensure that the force was adequately prepared, led, and controlled during Joint operations. Force warning time could be increased with systems that effectively disseminate intelligence data and command guidance. The force could then better utilize the precious time needed before hostilities for preparation, training, reconstitution, deployment, etc.

Factor Force

The tangible aspects of size and equipment, as well as the intangible aspects of training and combat readiness are also influenced by the degree of C4I interoperability among the force. The force size directly correlates to the amount of equipment it carries. Often specialists are required to operate intricate C4I systems and the devices that connect these systems. Interoperability of these systems can help to reduce equipment loads, thus reducing the manpower requirement. Transportation demands are reduced with decreased personnel and equipment requirements. Training cycles can be reduced and combat readiness increased with a force that is not constrained by having to learn about other service's systems and the workarounds inherent in attempting an interoperable link.

Interviews and correspondence with several professionals from CENTCOM, technical industry, and academic venues reveals a common story.¹⁹ The impact on the user of systems that are not interoperable is dramatic. Typical comments include:

- There is no Joint standard for systems interoperability.
- System workarounds are the rule, and too much is done on the fly.
- There are very few engineers left in government who have the technical know-how to understand emerging systems.
- Leaders charged with procuring C4I systems must be technically proficient.
- Our current C4I systems have some significant limitations in their ability to support the full range of operations that we may be tasked to undertake due to their lack of interoperability.
- C4I limitations include technical shortfalls, lack of requisite human skills, and an overall shortage of numbers (in platforms and people).
- Too many agencies are doing C4I procurement, so too many systems are developed and fielded.
- C4I interoperability enforcement has no teeth. The “hammer”: DISA is not focused on the problem; the Joint Staff is not funded to take care of the problem; the JROC probably has the power to take care of the problem, but is not focused on it just yet.
- The Services shouldn't have to live with disparate systems.
- It takes too long to get C4I systems fielded, and it is almost impossible to kill a program once it is underway.

These comments illustrate that a critical operational imperative for the JTF Commander is a clear understanding of the capabilities and limitations of his C4I support. Critical to successful command and control is an ability to understand the range of uncertainty about enemy operations through the use of C4I technology, and to effectively manage that uncertainty.

SOLUTION

The solution to the C4I systems quandary is interoperability assurance. A critical element of interoperability assurance is a clear prescription of a common suite of capabilities that must be inherent in all C4I systems that desire to interoperate. Each C4I system must cover all four enabling attributes of interoperability: procedure, applications, infrastructure, and data. At

¹⁹ Steve Mieir and Jeff Terry, United States Central Command (J6); Drew Hamilton, Auburn University; Bill Kemple, Naval Postgraduate School, Joint C4I, telephone conversations with author, April 2002.

each level of interoperability, DoD must identify a common suite of capabilities across procedure, applications, infrastructure, and data that must be incorporated by system developers in order to have a common-ground basis for Joint interoperability assurance. Finally, common standards must be adhered to for each capability.

DoD Services and Agencies can receive direct benefits from applying this mind-set. JTF planners, program managers, and system evaluators are but a few of the users that can realize increased mission effectiveness, appreciable return on investment, and reduction in system development costs. Operational planners can see increased mission effectiveness by reducing JTF set-up time due to early identification of C4I interoperability gaps and shortfalls. Services and Agencies can realize a return on the costs associated with ensuring their C4I systems are interoperable through early detection and resolution of interoperability gaps or shortfalls. And finally, all of DoD can accomplish a reduction in system development costs by leveraging off of previously fielded, certified C4I interoperable systems.

The CJCS must direct the Joint Staff, in collaboration with the regional CINCs, the Services, and the Director of DISA, to develop a process for prioritizing C4I systems for testing and certification. Further, the CJCS must direct the Joint Staff to develop a formal process to follow up on interoperability problems observed during exercises, report the problems to the relevant DoD organization, and inform organizations that the systems are required to be tested for interoperability. The “hammer” responsibilities must reside with an organization with authority and will, like the Joint Staff. In general, the C4I systems must be prioritized by importance to the CINCs, interoperability standards articulated, and certification progress assessed.

Specifically, the “hammer” must pick the C4I system “best of breed,” fix that system so it interoperates with all of the Services and does what the Services want it to do, and kill the acquisition of other like systems, thus concentrating on the winner. In addition, the links for these systems can help ensure interoperability by allowing only certified systems to have access to the network. This will help to ensure that the systems integrate as well as interoperate. In other words, a C4I system can interface with the “Joint Pipe” only if it abides by the interoperability standards of the connection.

CONCLUSION

The operational factors of space, time, and force are enhanced by the use of interoperable C4I systems by the operational commander. We must be more focused on the tangible military benefit to the operational commander, not on ensuring that the military/industrial complex remains afloat or a Service’s “pet project” makes it through the acquisition cycle. This can be accomplished through defense industrial cooperation. DoD development and manufacturing programs can be designed to demonstrate sharing in C4I systems technology and architecture, and leverage interoperability initiatives. Technology and architecture sharing can be monitored to ensure the systems are developed to a predetermined and agreed upon level that is commensurate with Service training levels. Joint experimentation can be mandated for each CINC and Service to ensure compliance with the standard and provide a medium for training. C4I interoperability will help ensure the DoD realizes true transformation, not simply evolution, during the current IT revolution.

BIBLIOGRAPHY

ASD, C3I Web Page <http://c3i.osd.mil>

Black, Michael. *Coalition C4I Systems Interoperability: A Necessity or Wishful Thinking?* Ft. Leavenworth: U.S. Army C&GSC, 2000.

C4ISR Architecture Working Group. *Levels of Information Systems Interoperability (LISI)*. 30 March 1998. http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdfdocs/lisi.pdf [6 April 2002].

Congress, Senate. *Congressional Record*, 99th Congress, 3 October 1958.

Defense Information Systems Agency (DISA) Web Site <http://disa.mil>

Department of Defense, Armed Forces Staff College. *The Joint Staff Officer's Guide 1991*. AFSC Publication 1. Washington: Government Printing Office, 1991.

Department of Defense, Joint Chiefs of Staff. *Joint Warfare of the Armed Forces*, Joint Publication 1. Washington: National Defense University Press, 1991.

DoD Directive 2010.6. *Standardization and Interoperability of Weapons Systems and Equipment within the North Atlantic Treaty Organization*. Washington: DoD, 1980.

DoD Directive 4630.5. *Compatibility, Interoperability, and Integration of C3I Systems*. Washington: DoD, 1992.

DoD Instruction 4630.8. *Procedures for Compatibility, Interoperability, and Integration of C3I Systems*. Washington: DoD, 1992.

DoD Instruction 5000.2. *Operation of the Defense Acquisition System*. Washington: DoD, 2001.

Hamilton, Drew. hamilton@Eng.Auburn.EDU “Joint C4I Interoperability” [E-mail to Patrick Kanewske kanewske@cox.net] 21 April 2002.

Joint Army and Navy Board. *Joint Action of the Army and the Navy*. Washington: Government Printing Office, 1927.

Joint Interoperability Test Command (JITC) Web Site <http://jitc.fhu.disa.mil>

Joint Publication 1-02. *DoD Dictionary of Military and Associated Terms*. Washington: DoD, 2001.

Joint Vision 2020. Washington: JCS, 2000.

Kemple, Bill. Naval Postgraduate School, Joint C4I Curriculum. Telephone conversation with author, 26 April 2002.

Lynch, Rick et al. *U.S. Army and Marine Corps Interoperability: A Bottom-up Series of Experiments*. Alexandria, VA: Joint Advanced Warfighting Program, 2000.

Mieir, Steve. CENTCOM, J6, Current Operations. Telephone conversation with author, 19 April 2002.

National Computer Security Center. *Introduction to Certification and Accreditation*. Ft. Meade: National Computer Security Center, 1994.

Office of the Inspector General. *Audit Report on DoD Participation in NATO Tactical C3 Interoperability*. Washington: DoD, 1992.

Paige, Jr., Emmett. *Retaining the Edge on Current and Future Battlefield Defense. Defense Issues*, August 1995.

Shalikashvili, John. *National Military Strategy – Shape, Respond, Prepare Now: A Military Strategy for a New Era*. Washington: CJCS, 1997.

Terry, Jeff. CENTCOM, J6, Plans. Telephone conversation with author, 22 April 2002.

United States General Accounting Office. *DoD's Renewed Emphasis on Interoperability is Important but Not Adequate*. Washington: GAO, 1993.

United States General Accounting Office. *Weaknesses in DoD's Process for Certifying C4I Systems' Interoperability*. Washington: GAO, 1998.

Vego, Milan. *Operational Warfare*. U.S. Naval War College, 2000.

Weigley, Russell. *The American Way of War*. Bloomington: Indiana University Press, 1973.

APPENDIX A

Interoperability Definitions and Terms²⁰

Common Operating Environment - Automation services that support the development of the common reusable software modules, which enable interoperability across multiple combat support applications. This includes segmentation of common software modules from existing applications, integration of commercial products, development of a common architecture, and development of common tools for application developers.

Global Combat Support System - A strategy that provides information interoperability across combat support functions and between combat support and command and control functions through the Global Command and Control System.

Interoperability - 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. (DOD only) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.

Joint Test Publication - A proposed version of a joint doctrine or joint tactics, techniques, and procedures publication that normally contains contentious issues and is nominated for a test publication and evaluation stage. Joint test publications are approved for evaluation by the Director, Operational Plans and Interoperability (J-7), Joint Staff. Publication of a test publication does not constitute Chairman of the Joint Chiefs of Staff approval of the publication. Prior to final approval as joint doctrine, test publications are expected to be further refined based upon evaluation results. Test publications are automatically superseded upon completion of the evaluation and promulgation of the proposed publication.

Rationalization - Any action that increases the effectiveness of allied forces through more efficient or effective use of defense resources committed to the alliance. Rationalization includes consolidation, reassignment of national priorities to higher alliance needs, standardization, specialization, mutual support or improved interoperability, and greater cooperation. Rationalization applies to both weapons and/or materiel resources and non-weapons military matters.

ADSIA - Allied Data Systems Interoperability Agency

CIWG - Communications Interoperability Working Group

FIA - Functional Interoperability Architecture

IAR - Interoperability Assessment Report

²⁰ Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, (Washington: DoD, 2001).

IDSS - Interoperability Decision Support System

IIP - Interoperability Improvement Program/Panel

IPS - Interoperability Planning System

ITP - Interoperability Test Panel

JAMPS - Joint Interoperability of Tactical Command and Control Systems (JINTACCS)
Automated Message Preparation System

JIEO - Joint Interoperability Engineering Organization

JIES - Joint Interoperability Evaluation System

JINTACCS - Joint Interoperability of Tactical Command and Control Systems

JITC - Joint Interoperability Test Command

JWID - Joint Warrior Interoperability Demonstration

NIEX - No-notice Interoperability Exercise

NIEXPG - No-Notice Interoperability Exercise Planning Group

RSI - Rationalization, Standardization, and Interoperability

TISG - Technical Interoperability Standards Group